




Operational Support Tool 300-00-06A

LANL Hazard Analysis Technical Methodology Handbook

Los Alamos National Laboratory

Developed by

Facility and Waste Operations Division
Office of Authorization Basis

Prepared by:	Signature:	Date:
Patrick McClure		3-19-01
Kent Sasser		3-19-01
Approved by:	Signature:	Date:
Kent Sasser, Office of Authorization Basis		3-19-01

HISTORY OF REVISIONS

Revision	Date	Summary
0	03/19/01	Original Issue

Table of Contents

1. Introduction	1
1.1 Purpose	1
1.2 Scope & Applicability	1
1.2.1 Scope	1
1.2.2 Applicability	1
2. Definitions	2
3. Requirements	5
3.1 Pre-Start Activities Applicable to all Hazard Analyses (HAs)	5
3.1.1 Baseline Information	5
3.1.2 Hazard Analysis Techniques	6
3.1.3 HA Team	6
3.1.4 Use of Frequency, Consequence, and Risk Matrices	7
3.2 Operational Phase What-If Hazard Analysis	14
3.2.1 HA Organization	14
3.2.2 Hazard Identification and Screening	16
3.2.3 Hazard Analysis	17
3.2.3 Hazard Evaluation and Selection of Formal Controls	22
3.2.4 Format and Content for Standalone Hazard Analysis	23
3.3 Preliminary Hazard Analysis for Project Design Phase	24
3.3.1 PHA Results Format	25
3.3.2 SSC Safety Functions and Functional Requirements	26
3.4 Hazard Analysis for Project Title I Preliminary Safety Document	29
<u>REFERENCES</u>	30
Attachment A: Hazard Identification Checklist	31
Attachment B: Estimating Accident Scenario Public Radiological Consequences	33
Attachment C: Guidance for Hazard Evaluation & Selection of Safety Controls	36

1. Introduction

1.1 Purpose

This handbook is intended to aid LANL safety analysts in producing consistent and technically sound hazard analyses (HA). It provides a common methodology to ensure consistency. It is a “how to” guide and a reference source for information needed for such work. Analysts that utilize methods described in this handbook are using a LANL ‘safe harbor’ method. These methods are more easily accepted and defended and, as such, more likely to be approved in a timely and cost effective manner.

1.2 Scope & Applicability

1.2.1 Scope

This handbook establishes the format and methodology to be used throughout the LANL site for performing the HA for safety basis (SB) documents. This includes Documented Safety Analyses (DSA) for nuclear facilities (also known as Safety Analysis Reports or SARs), Bases for Interim Operations (BIOs), Facility Safety Analyses (FSA) for non-nuclear facilities, or other needs for an HA. This methodology is also consistent with the LANL Safe Work Practice (SWP) process and the Integrated Safety Management (ISM) program. Note, however, Hazard Control Plan documentation is prepared using the SWP requirements.

The HA process:

- Identifies and describes the work to be performed
- Systematically identifies hazards
- Determines the unmitigated consequences of abnormal occurrences or accidents
- Identifies the measures taken to eliminate, control, or mitigate the hazards
- Evaluates the adequacy of those measures; identifying the structures, systems, and components (SSCs) and controls that are important to safety.

Important controls may become candidates for designation at a higher level, e.g. Safety Significant or Safety Class for nuclear facilities. These controls will have associated with them the appropriate level of formality (e.g., Technical Safety Requirements) depending on the purpose of the HA.

The HA methodology discussed in this document considers hazards, including natural phenomena, that can initiate and contribute to the uncontrolled releases of radioactive or hazardous materials, or any significant hazard (other than Standard Industrial Hazards) that can significantly impact the public or workers. It does not consider sabotage or terrorism.

1.2.2 Applicability

The HA methodology described in this handbook is applicable for the following:

- Safety Basis for nuclear facilities that are operational, in accordance with 10CFR 830, LIR-300-00-06, DOE STD 3009, STD 3011, or other applicable standards.

- Safety analyses for construction project authorization throughout the life cycle from project conceptual design to approval for operations, to meet LIR-220-01-01 requirements
- Safety Basis for non-nuclear facility authorization, as defined in LIR-300-00-07.
- Any need to fully evaluate hazards using a methodology accepted by industry and DOE standards, consistent with the LANL SWP process

2. Definitions

The following definitions, to the extent possible, were taken from appropriate DOE rules and regulations, e.g. 10 CFR 830 (ref. 9) and DOE STD 3009 (ref. 7).

Accident – an unplanned sequence of events that results in undesirable consequences.

Accident Analysis - for the purposes of implementing 10 CFR 830 and DOE Std 3009, the term accident analysis refers to those bounding analyses selected for inclusion in the SAR or DSA. These analyses refer to design basis accidents only. Accident analysis has historically consisted of the formal development of numerical estimates of the expected consequences and probability of potential accidents associated with a facility. For the purposes of implementing DOE Std 3009, accident analysis is a follow-on effort to the HA. As such, it requires documentation of the basis for assignment of likelihood of occurrence (e.g. 1/yr to 10^{-2} /yr) and performance of a formally documented consequence analysis. Consequences are compared with offsite Evaluation Guidelines to identify safety class structures, systems, and components (SSC).

Administrative Controls – the provisions relating to organization and management, recordkeeping, assessment, and reporting necessary to ensure safe operation of a facility.

Design Basis – the set of requirements that bound the design of SSCs within the facility. These design requirements include consideration of safety, plant availability, efficiency, reliability, and maintainability. Some aspects of the design basis are important to safety, others are not.

Design Features – the design features of a (nuclear) facility specified in the technical safety requirements that, if altered or modified, would have a significant effect on safe operation.

Documented Safety Analysis (DSA)– a documented analysis of the extent to which a facility can be operated safely with respect to workers, the public, and the environment, including a description of the conditions, safe boundaries, and hazard controls that provide the basis for ensuring safety. The DSA, as defined in 10CFR830, is a new term which is considered to be the same as the term Safety Analysis Report as defined in DOE Standard 3009.

Facility Safety Analysis – A safety analysis and determination of controls for nonnuclear Category A and B facilities.

Graded Approach – the process of ensuring that the level of analysis, documentation, and actions used to comply with a requirement are commensurate with

1. The relative importance to safety, safeguards, and security;
2. The magnitude of any hazard involved;
3. The life cycle stage of the facility;

4. The programmatic mission of the facility;
5. The particular characteristics of the facility;
6. The relative importance of radiological and nonradiological hazards; and

Hazard – a source of danger (i.e. material, energy source, or operation) with the potential to cause illness, injury, or death to a person or damage to a facility or to the environment (without regard to the likelihood or credibility of accident scenarios or consequence mitigation).

Hazard Analysis – The determination of material, system, process, and plant characteristics that can produce undesirable consequences, followed by the assessment of hazardous situations associated with a process or activity. Largely qualitative techniques are used to pinpoint weaknesses in design or operations of the facility that could lead to accidents. The Documented Safety Analysis HA examines the complete spectrum of potential accidents that could expose members of the public, onsite and facility workers, and the environment to hazardous materials.

Hazard Controls – measures to eliminate, limit, or mitigate hazards to workers, the public, or the environment, including

1. Physical, design, structural, and engineering features,
2. Safety structures, systems, and components,
3. Safety management programs,
4. Technical Safety Requirements, and
5. Other controls necessary to provide adequate protection from the hazards.

Mitigative Feature - any structure, system, or component that serves to mitigate the consequences of a release of hazardous material in an accident scenario.

Nonreactor nuclear facility – facilities, activities, or operations that involve, or will involve, radioactive and/or fissionable materials in such form and quantity that a nuclear or nuclear explosive hazard potentially exists to workers, the public, or the environment, but does not include accelerators and their operations and does not include activities involving only incidental use and generation of radioactive materials or radiation such as check and calibration sources, use of radioactive sources in research and experimental and analytical laboratory activities, electron microscopes, and X-ray machines. [10CFR830].

Preliminary Documented Safety Analysis – documentation prepared in connection with the design and construction of a new DOE nuclear facility or major modifications to a DOE nuclear facility that provides a reasonable basis for the preliminary conclusion that the (nuclear) facility can be operated safely through the consideration of factors such as

1. The nuclear safety design criteria to be satisfied,
2. A safety analysis that derives aspects of design that are necessary to satisfy the nuclear safety design criteria, and
3. An initial listing of the safety management programs that must be developed to address operational safety considerations.

Preventive Feature - any structure, system, or component that serves to prevent the release of hazardous materials in an accident scenario.

Process Safety Management (PSM) - a process or activity involving the application of management principles as defined in 29 CFR 1920. 119, “Process Safety Management of Highly Hazardous Chemicals”.

Public - all individuals outside the DOE (LANL) site boundary.

Safety Basis – the documented safety analysis and hazard controls that provide reasonable assurance that a DOE (nuclear) facility can be operated safely in a manner that adequately protects workers, the public, and the environment [10 CFR 830]. Note: In the past, the term Authorization Basis has been used to represent the same set of documents and controls as the Safety Basis. At LANL, the term Safety Basis will be used, however, recognizing that many older documents will continue to be used until those documents are revised.

Safety Class Structures, Structures, and Components – the SSCs, including portions of process systems, whose preventive or mitigative function is necessary to limit radioactive hazardous material exposure to the public, identified in the DSA.

Safety management program – a program designed to ensure a facility is operated in a manner that adequately protects workers, the public, and the environment by covering a topic such as: quality assurance; maintenance of safety systems; personnel training; conduct of operations; inadvertent criticality protection; emergency preparedness; fire protection; waste management; or radiological protection of workers, the public, and the environment.

Safety Significant structures, systems, and components – the structures, systems, and components which are not designated as safety class structures, systems, and components, but whose preventive or mitigative function is a major contributor to defense in depth and/or worker safety as determined from the DSA Hazard Analysis.

Safety SSCs - safety class or safety significant SSCs.

Site Boundary - a well marked boundary of the property over which DOE and LANL (owner and operator) can exercise strict control without the aid of outside authorities. For safety basis purposes, the LANL site boundary is the geographic boundary within which public access is controlled and activities are governed by DOE and LANL, and not by local authorities. Any public road traversing the site is considered to be within the site boundary if, when necessary, DOE or LANL has the capability to control the road during accident or emergency conditions.

Standard Industrial Hazards (SIH) – hazards that are routinely encountered in general industry and construction, and for which national consensus codes and/or standards (e.g., OSHA, transportation safety) exist to guide safe design and operations without the need for special analysis to define safe design and/or operational parameters.

3. Requirements

3.1 Pre-Start Activities Applicable to all Hazard Analyses (HAs)

The following activities need to be completed prior to starting an HA:

- gather baseline information,
- determine the appropriate HA technique,
- identify a HA team, and
- define the frequency, consequence and risk matrices.

3.1.1 Baseline Information

Baseline information is the basic information needed to complete an HA. The HA success depends directly on the quality of information available. This information should be documented in such a way that it can be revised as information is updated. This will allow the HA to be updated with each design phase for a design & construction project or if the HA is revised at a later date. Facility design information should be accurate in accordance with LANL configuration management requirements. The following areas and associated information should be included as part of the baseline information and documented in a facility or process description portion of the HA:

Area 1. Facility/design information

- Facility description and drawings
- Materials of construction
- Building layout
- Facility plot plan/building drawings
- Facility systems and utilities
- Building penetrations

Area 2. Process/activity/operational information

- Piping & instrument diagrams (P&IDs)
- Process flow diagrams
- Instrumentation & controls
- Design bases for vessels/piping
- Design of relief systems (relief systems setpoints, etc)

Area 3. Materials & Hazards Information

- Hazard type (material, energy source, or action)
- Hazard form and quantity (mass, volume, pressure, temperature, composition, etc.)
- Hazard location and containment (room(s) or exterior locations)

Area 4. Existing Safety Documents

- Safety analysis reports
- Hazard analyses, fire hazard analyses
- Environmental reports
- Safety management reports
- Unreviewed Safety Question Determinations (positive and negative)
- Technical Safety Requirements (TSRs)

Area 5. Operations Information

- Historical occurrences, equipment reliability (failure data)
- Operations procedures, training, limits/controls

Area 6. Site and Location Characteristics

- Site characteristics
- Meteorology, seismic, site hydrology, other applicable natural phenomenon
- Distances to public boundaries, adjacent facilities
- Population of workers involved and not involved in the work

3.1.2 Hazard Analysis Techniques

The HA technique will depend on the type and complexity of the process or activity analyzed along with the facility life cycle stage. Three techniques are suggested for use. Reference 1 is a good source that describes these and other techniques and when they are most appropriate.

1. **What-If:** The most common and recommended HA technique used at LANL. This technique is most useful for systems of limited complexity. This method relies heavily on using a knowledgeable and experienced analysis team.
2. **Failure Modes and Effects Analysis (FMEA):** Used to identify equipment and hardware failures. To apply the FMEA technique, failures of hardware components of a system are postulated and their effects are determined. The FMEA can be used in conjunction with the What If method.
3. **Hazard and Operability Studies (HAZOPs):** A systematic way to examine how process variations affect a system. This technique is widely used in the chemical industry where there are continuous process systems. Due to the nature of work done at LANL, it is expected this technique will rarely be utilized.

The What-IF method is the most commonly used technique used at LANL. Key aspects of this technique that need to be adhered to in order to assure its successful and consistent application at LANL are provided in the following subsections.

3.1.3 HA Team

One of the first steps in performing a HA is to organize the HA team. The criteria for selecting a team and holding team meetings are discussed below.

Team Selection

The ideal team is a mix of individuals thoroughly familiar with the process or operations being evaluated, one or more safety analysts, and an experienced team leader.

- (1) **HA Team Leader.** The team leader has the overall responsibility for the HA. He/she brings organizing, planning, directing, and leadership skills to the effort. He/she is the primary interface with higher levels of management. The team leader should also be certified through HA team leader training or through demonstrated experience.
- (2) **Safety Analyst(s).** One or more safety analysts are members of the team. Safety analysts are experienced in performing analyses of this kind, identifying hazards, evaluating and estimating likelihood and consequences, and understanding what types of controls are normally employed and are effective. Depending on the type of facility or process, safety

analysts will be needed in specific disciplines, e.g. radiological, chemical, explosives, fire hazards, seismic analysis, and so on.

- (3) Systems or Design Engineer. Many facilities employ systems engineers to ensure that facility systems are designed, operated, and maintained correctly. These engineers should be thoroughly familiar with the facility, its systems, and their operational parameters.
- (4) Operations specialists. A facility operator is important to bring an understanding the facility operational history and current operational practices including effective means to prevent or mitigate an accident. An experienced operator will have first hand knowledge of whether a postulated failure or accident has actually occurred. Worker involvement is always required if the HA is being performed to meet Process Safety Management (PSM) rules¹.

At a minimum the HA should consist of a team leader, who can also be a safety analyst, and operations and engineering specialists. One individual should serve as the team scribe, to record the ongoing results of the team sessions (see below) and to keep the results updated. If the HA is performed as a part of an overall effort, e.g. a SAR or DSA, the HA Team Leader may report to a Project Manager. Normally a Project Manager is employed to ensure that the entire SB effort is completed according to standards, within budget, and on time.

Team Meetings

Team meetings are important to provide a synergistic mechanism for the team to conduct an HA. Facilitated by the team leader, a series of interactive team meetings should be held with all the team members in attendance. This issue of completeness of an HA (i.e., whether or not all the hazards have been identified and analyzed) is very important. These meetings give confidence to all the parties involved (including reviewers) of having done a thorough and accurate analysis.

Alternative methods such as assigning the HA to a single safety analyst most often produce less than satisfactory results. It is not acceptable for safety analysts to perform the HA in an isolated manner without the operational/facility expertise directly involved. In the context of an interactive team meeting, led by an experienced team leader, each segment of the facility or process can be evaluated and parameters such a consequences, likelihood, and controls can be identified accurately the first time. The team consensus in such an interactive team meeting is almost always the correct answer. Infrequently, the team leader may have to table a scenario or make assignments for a team member to collect additional data to complete scenario.

3.1.4 Use of Frequency, Consequence, and Risk Matrices

In the HA a set of accident scenarios are identified that could potentially cause harm to the public, worker, and/or environment. Each of these scenarios is assigned a frequency and consequence bin. Based on the assigned frequency and consequence bins, the risk bins are then determined. The range of values for each of the bins as well as the number of bins to use in an analysis is arguably very subjective. In fact, Standard 3009 stresses that what is important is the ability to rank scenarios in a relative manner, which can be done with any set of matrices. However, for many reasons, a set of standard matrices is being provided for use across LANL. Some of the benefits of using consistent matrices at LANL are;

¹ Process Safety Management of Chemical Materials, 29CFR1910.119

- Facilities and processes across the laboratory can be compared.
- Other processes dependent on the HA, such as the USQ process, can be easily standardized.
- Minimize conflict among analysts and reviewers as to how the matrices should appear, saving time, money, and energy that can be more efficiently used in doing the analyses.
- Analysts across the laboratory will be speaking the same “language” which will help in discussing topics as well as making it easier for analysts to work at different facilities.
- Matrices are consistent in terminology and bins with Safe Work Practices.

The following matrices are provided:

- Table 1, frequency or likelihood matrix
- Table 2, public consequence binning matrix
- Table 3, facility worker consequence matrix
- Table 4, risk matrices for the public
- Table 5, risk matrices for the workers

Guidelines For Use of HA Matrices

DOE-STD-3009 advocates that the team determine necessary controls to adequately protect the workers based on the results of HA which is typically qualitative. The matrices are also intended facilitate selection of accidents for performing accident analysis. Since the accident analysis is done for determination of safety class SCCs using the offsite EG as a guideline, the use of a matrix is, therefore, also intended for protection of the public. Some guidelines, developed through past interactions with DOE are as follows:

1. The matrix should NEVER be the decision maker. A matrix is not sophisticated enough to replace sound engineering logic. Therefore, it is important to recognize that the matrix only provides useful information to LANL/DOE to aid in decision making.
2. Matrices should not be used to determine the safety importance of SSCs (i.e. not to be used to designate Safety-Significant or Safety-Class SSCs). STD-3009 advocates an approach based on engineering logic to make these classifications.
3. Risk matrices should not make statements about acceptable risk.
4. A distinction must be made in risk to the public and the worker. They cannot be equated.
5. The use of risk matrixes for worker protection may be more challenging than its use for the public since the accident parameters (i.e., source term, distance factors) for the workers (a close proximity of the workers to an accidental source) are more uncertain than those associated with the more distant public.
6. There is no intent to perform "accident analysis" for the worker. Most calculations for the worker are impractical. They are not a part of DOE guidance.
7. Risk ranking should not circumvent the HA process. In other words, low initial risk is not an excuse to screen out or delete the scenario from the HA. The HA is complete, the lower rankings may result in fewer requirements for controls.
8. USQ process needs to maintain a distinction from risk matrices (i.e. not to be driven by iso-risk argument. Example, just because a new activity has the same or lower risk (i.e. same risk rank or consequence times frequency) does not mean it is not a positive USQ.

Table 1 Frequency Matrix

I ($>10^0/\text{yr.}$)	FREQUENT (expected)	Likely to occur <u>often</u> during the life of the facility. (Incidents that occur during normal operation)
II ($<10^0/\text{yr.}$ to $>10^{-2}/\text{yr.}$)	PROBABLE (likely)	Likely to occur <u>several times</u> during the life of the facility. (Incidents that may occur during the lifetime of the facility; these are incidents with a mean expected likelihood of once in 50 years)
III ($<10^{-2}/\text{yr.}$ to $>10^{-4}/\text{yr.}$)	OCCASIONAL (unlikely)	Should not occur during the life of the facility. (Incidents that are not anticipated to occur during the lifetime of the facility but could; these are incidents having a likelihood of between once in 100 years to 10,000 operating years)
IV ($<10^{-4}/\text{yr.}$ to $>10^{-6}/\text{yr.}$)	IMPROBABLE (extremely unlikely)	Unlikely but possible to occur during the life of the facility. (Incidents that will probably not occur during the lifetime of the facility; these are incidents having a likelihood of between once in 10,000 years and once in a million years)
V ($<10^{-6}/\text{yr.}$)	REMOTE (beyond extremely unlikely)	Should not occur during the life of the facility. (All other incidents having a likelihood of less than once in 1,000,000 operating years)

Table 2
Public Consequence Severity Binning Table

CATEGORY	DEFINITION
A	<p><u>Offsite DOE EG or EPA Exposure Guidelines Exceeded or Challenged:</u> Potential for long-term health effects.</p> <ul style="list-style-type: none"> ● >25 Rem TEDE (DOE EG per Appendix A to DOE-STD-3009) ■ .>ERPG-2
B	<p><u>Offsite DOE EG or EPA Exposure Guidelines not Exceeded but may be Challenged:</u> Produces irritation or discomfort but no permanent health effects.</p> <ul style="list-style-type: none"> ● From >5 to <25 Rem ■ From >ERPG-1 to <ERPG-2
C	<p><u>No Challenge to Offsite DOE EG or EPA Exposure Guidelines:</u> No significant off-site impact.</p> <ul style="list-style-type: none"> ● From .>0.1 to <5Rem ■ From measurable to <ERPG-1
D	<p><u>Negligible :</u> No off-site impact</p> <ul style="list-style-type: none"> ● < 0.1 Rem (Offsite life-time dose per year per DOE-O-5400.5) ■ < measurable
E	<p><u>None</u> (Can elect not to use this bin if desired)</p>

Legend:

- Radiological Hazards
- Chemical Hazards

EG Evaluation Guideline (25 Rem) at site boundary (i.e., the MOI);
ERPG Emergency Response Planning Guideline at site boundary (i.e., the MOI);

Table 3
Worker Consequence Severity Binning Table²

CATEGORY	DEFINITION
A	<u>Immediate Health Effects or loss of life</u>
B	<u>Long-term health effects, disability, or severe injury (non life threatening)</u>
C	<u>Lost-time injury but no disability (work restriction)</u>
D	<u>Minor injury with no disability and no work restriction</u>
E	<u>No measurable consequences</u>

² Worker normally refers to ‘facility’ worker. This consequence matrix may be used also if the team needs to evaluate the consequences to what has been referred to as the co-located worker, located at some distance from the work site or in adjacent facilities on-site.

Table 4: Public Hazard Risk Matrix**F R E Q U E N C Y**

Decreasing Likelihood ---->

		I	II	III	IV	V
C O N S E Q U E N C E	A	1	1	2	2	3
	B	1	2	2	3	3
	C	1	2	3	3	4
	D	3	3	3	4	4
	E	4	4	4	4	4

Increasing Severity --->

† Dashed boundary between Risk Rank 2 and 3 follows the proposed DOE-DP off-site public guideline in "Method for Assessment of Worker Safety Under Radiological Conditions at DOE Nuclear Facilities," US. DOE, Office of ES&H, EH-12-94-01, June 1994.

Table 5
Worker Hazard Risk Matrix

F R E Q U E N C Y

←----- Increasing Likelihood

		I	II	III	IV	V
C O N S E Q U E N C E	A	1	1	2	2	3
	B	1	1	2	3	4
	C	1	2	3	4	4
	D	2	3	4	4	4
	E	4	4	4	4	4

Increasing Severity --->

3.2 Operational Phase What-If Hazard Analysis

This section describes the What-If HA for a facility that is operational or about to enter the operational phase after completion of construction and readiness assessment. There are several logical steps to be followed to the extent possible and appropriate. HAs for simple facilities or processes may complete these steps in an abbreviated fashion or can skip a step if appropriate.

3.2.1 HA Organization

General steps for organizing the HA are provided in this section.

Define Scope of Analysis

Typically, the scope encompasses an entire complex, facility, or process line, often defined within some boundary, e.g. TA-55 fence. The scope may include adjacent facilities and activities to the extent that they affect the subject facilities, facility or process. The scope could include activities such as transportation (internal or external to the facility), waste management, or other support activities.

It is extremely important to clearly define the scope prior to starting. This is particularly true for an HA for a SAR type document, as the accident analysis builds on the HA. Changing the scope results in repeating steps of the HA with additional costs and time. For LANL AB processes, a 0% scoping meeting has been incorporated into the project process to ensure that all involved parties agree on the scope of the AB, beginning with the HA.

Grouping or Organization of the Physical Facility or Major Processes

The physical facility or major processes within the HA scope should be grouped in a fashion that allows activity specific hazards to be identified. Each facility usually has a very logical way to be organized for the HA. An example facility or process summary is shown as Table 6.

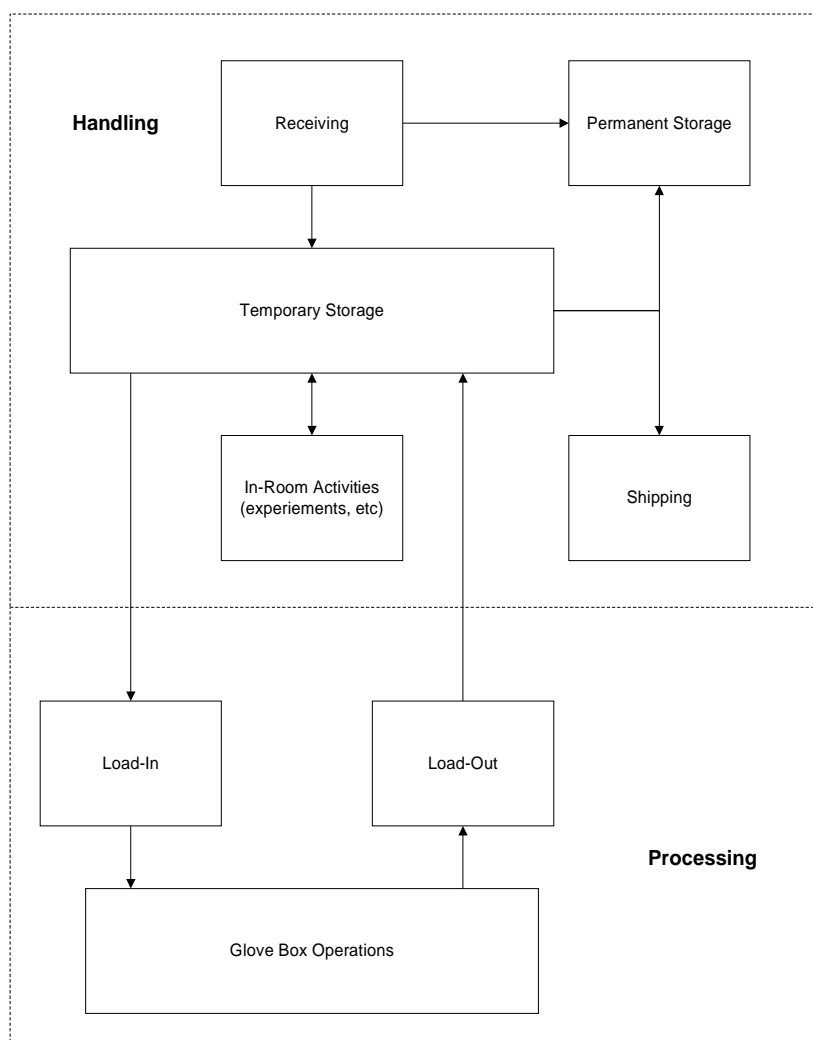
As an aid in determining the significant physical arrangements or major process steps that should be identified and analyzed, it is useful to construct one or more simple block or process diagram illustrating the flow of hazardous or process materials through a facility or line. Block diagrams are an excellent way to organize the scope into the various segments. Each segment can be further flow charted into activities if appropriate. An experienced team leader will provide the first attempt with final forms developed in team meetings. Sometimes physical grouping is most appropriate, other times separation by major processes is more appropriate. Reference 1 provides worked examples along with flowcharts. Examples of block diagrams that show major processes in a facility are shown in Figures 1 and 2.

Link Activities to Physical or Process Segments

The previous section described how the facility is organized into manageable segments. Most often this is by physical location, other times it makes more sense to break into major process segments, again this is determined through the team leader/team interactions. The identified activities should be linked to the segments in which they are conducted. Table 7 illustrates a sample matrix in which activities are linked to the physical areas of facility.

Table 6. Example Process Summary for FACILITY X

Activity No.	Description
1	Receiving
2	Permanent Storage
3	Temporary Storage
4	Bench-top Experiments
5	Load In to Process Line
6	Process Line Operations
7	Load Out of Process Line
8	Shipping

**Figure 1. Example Block diagram of processes in FACILITY X.**

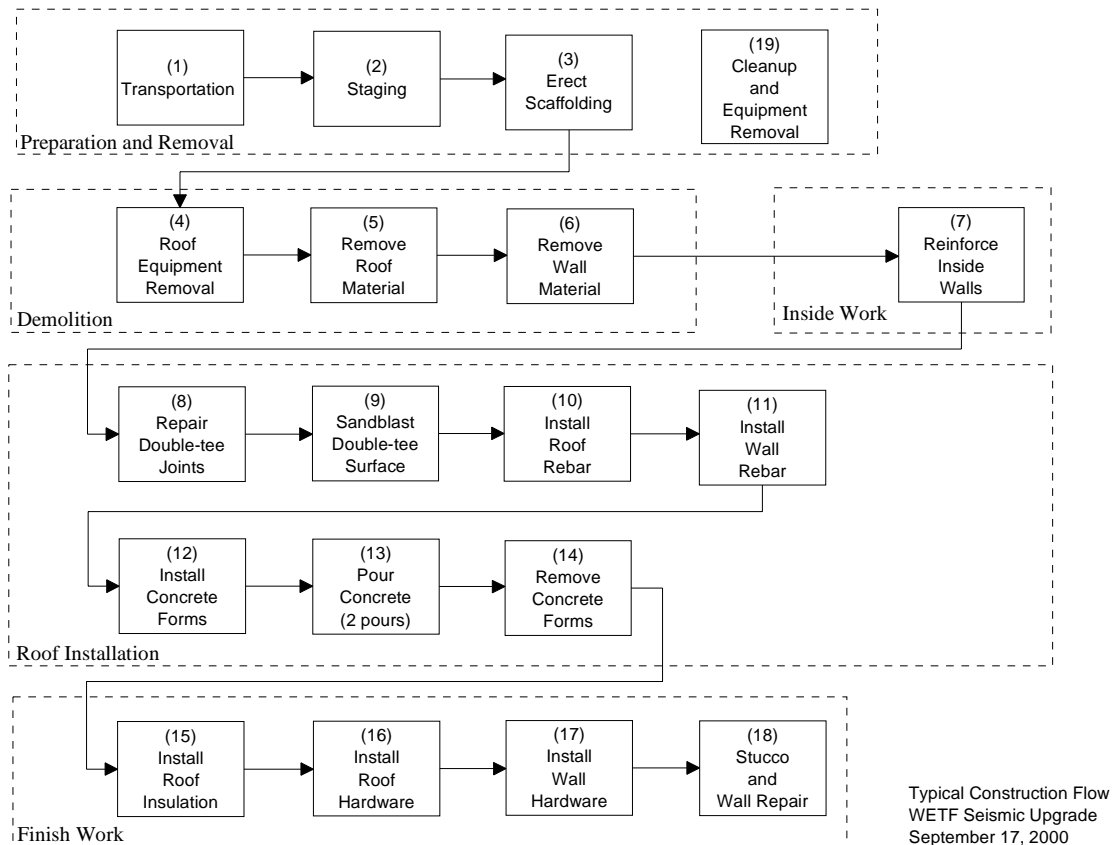


Figure 2. Example Block diagram of facility modification process segments and activities.

3.2.2 Hazard Identification and Screening

The hazard identification process involves several steps:

- Identifying all facility/process hazards using the checklist as an aid
- Determining whether the identified hazards are to be evaluated (Screening)

A hazards identification checklist is useful to use in reviewing the range of possible hazards found in the facility or activity being evaluated. Checklists have been compiled by various sources. An example of a useful checklist is provided in Attachment A (taken from Ref. 1). The use of this checklist is strongly encouraged although others may be used if defensible.

Table 7 – Sample Matrix Linking Activities to Location or Process

Activity	Area or Process 1	Area or Process 2	Area or Process 3	Area or Process 4	Area or Process 5	Area or Process 6
1	X	X	X	X	X	X
2	X	X	X	X	X	X
3			X	X	X	
4			X	X	X	
5		X	X	X	X	
6			X	X	X	X
7		X	X	X	X	
8	X	X	X	X	X	X

For each segment and activity developed, hazard identification is performed using the checklist. The team can use the checklist during facility walkdowns, interviews of operations staff, and reviewing facility procedures or existing safety documents. The inventories of hazardous materials and energetic sources are listed and consolidated. The checklist provided in Attachment A also has space to record the hazards found along with inventories and locations.

After completing a complete inventory of the facility hazards, the HA team should perform a hazard review. Depending on the requirements for the HA some of the hazards may be deleted from further consideration. For example, for a nuclear facility SAR hazard analysis, DOE STD 3009 allows deleting Standard Industrial Hazards, unless those hazards could lead to the release of radiological or toxic materials. All hazards not screened are retained for study. If there is any unresolved question as to the need to include the hazard, the process hazard should be passed on to the more detailed HA step.

3.2.3 Hazard Analysis

This section describes the HA process to evaluate the identified facility or project hazards using the What-If technique. This section provides the following:

- a standard format to present the results of the HA.
- how the hazard/accident scenarios are determined.
- how the controls are identified.
- guidance on determining accident scenario frequencies.
- a method to estimate the consequences of radiological and chemical releases

Results Format

The HA should be documented in tabular form. The format in Table 8 should be used. An alternate table can be used, but it must provide the same information. The table includes several example scenarios. The table is constructed to provide key information on each parameter of an accident that is important. Each column should be completed for each accident scenario to the fullest extent possible. Each column is described below. As the information is derived in the team session, the team scribe should record the information, ultimately formatting it in the

format of this table. For example, a simple What If form can be used in the team analysis, but the data on Table 8 needs to be ultimately developed.

1. #: The unique identifying number given to the accident scenario, usually tied to the HA segment, location, or activity
2. Hazard: The hazard being analyzed (e.g., Pu, U, TRU Waste, Tritium, etc.)
3. Accident Type: The accident type being evaluated. There are normally a few basic accident types to choose from: (fire, spill, explosion, criticality, external event, natural phenomenon). Be consistent in order that the results later can be electronically or manually sorted by type for evaluation.
4. Scenario: Provide brief description of the accident scenario. This includes the accident initiator, progression of the accident, and narrative conclusions of consequences.
5. Uncontrolled Likelihood Bin: The unmitigated likelihood (frequency) without regard for preventive controls.
6. Uncontrolled Consequence Bin: The unmitigated consequence without consideration of preventive or mitigative controls.
7. Existing Controls: Existing controls that the teams feels can be effective in preventing or mitigating the accident. Use a unique identifier for each engineered (EC), administrative (AC), or passive (P) control. Each of these controls is then listed in a separate table where a more full description of the control and its safety functions can be described. Table 9 is an example of the companion listing of controls. Each control is also determined to be either primarily a preventor or mitigator.
8. Controlled Frequency: The mitigated frequency considering the controls available.
9. Controlled Consequence: The mitigated consequence considering the controls available.
10. Uncontrolled Qualitative Risk: Risk to public and workers without controls.
11. Controlled Qualitative Risk: Risk to public and workers with controls considered.

Identifying Hazard/Accident Scenarios

In a series of team sessions facilitated by the team leader, the entire team should begin the task of identifying accident scenarios of interest. Using the material developed in the previous section, the team evaluates the facility one segment at a time. The team leader may have prepared beforehand a set of starting accidents and/or What If questions. During the session, the team will evaluate the normal operations, postulating upsets or accident conditions one segment at a time.

For example, when handling a drum of toxic materials the team could postulate a number of accident conditions, for example:

- Drum has deteriorated and begins to leak during handling
- Operator drops drum causing breach and release of toxic materials
- Crane/forklift accident causes rupture.
- Drum energetic failure (if contents could have caused pressure buildup)
- Drum contaminated from failure during storage
- Fire caused by events during handling causes toxic material release

Table 8
Completed HA Results

(linked to process flowchart, scenarios listed are for example purposes)

Preparation & Transportation (THIS IS THE SEGMENT FROM THE PROCESS FLOW)

#	Hazard	Accident type	Scenario	Uncontrolled		Controls		Controlled		Qualitative Risk		Notes
				Likelihood Bin	Consequence Bin	Existing	Recommended	Likelihood Bin	Consequence Bin	Uncontrolled	Controlled	
1	Tritium	Transportation Accident	Construction vehicle strikes site electrical substation or electrical distribution pole guy wire causing an electrical fault, causing loss of site power. No release of tritium from building expected.	III	W = E P = E	1. Bollards (EC-1) 2. Diesel Generator (EC-2) 3. UPS (EC-3) 4. Inventory Control (AC-13)	1. limit or define traffic pattern	IV	W = E P = E	W = 4 P = 4	W = 4 P = 4	App. B Refs 1 & 2 estimate truck accident rate with object from 15E-6/mile to 1 E-6/mile. Multiple trucks (50-100) for construction. Likelihood conservatively chosen as III.
3	Tritium	Transportation Accident, large Fire, Tritium release (up to 650 g)	Construction vehicle strikes diesel fuel tank, rupturing tank. Major fire, from diesel fuel spill is initiated in the equipment room area. Unmitigated the fire engulfs the building and spreads to other buildings where tritium stored (large fire)	III	W = A P = A	1. Bollards (EC-1) 2. Diesel Tank Wall (EC-4) 3. Bldg 205 Masonry block wall isolation (EC-5) 4. Bldg Fire Protection System (EC-7) 5. Bldg fire barriers (EC-6) 6. Combustible control program (AC-1) 7. Tritium Monitoring System (EC-8) 8. Evacuation Training (AC-2) 9. Emergency Plan (AC-3) 10. Contractor AHA (AC-6)	1. limit or define traffic pattern 2. Spotter when maneuvering near building or tanks.	V	W = D P = E	W = 2 P = 2	W = 4 P = 4	In addition to Note in Scenario #1, Ref 1 gives conditional probability for rupture of tank and causing fire as E-4. Bins conservatively chosen high.

Table 9 List of Identified Controls (linked to HA Table)

(controls are listed as examples only)

Identifier	Control	Preventive (P), or Mitigative (M)	Discussion
Engineered Controls			
EC-1	Bollards	M	Concrete filled steel pipes imbedded in the ground at a separated distance from the structure of concern acts as a primary defense from moving vehicles.
EC-2	Diesel Generator	M	The diesel generator starts and provides power to loads about 20 seconds after a power interrupt.
EC-3	UPS	M	An uninterruptable power supply monitors incoming distribution or diesel power for upsets and provides temporary power for up to 30 minutes.
EC-4	Diesel Tank Wall	P	Diesel storage tank has double wall, concrete reinforced construction
EC-6	Building Fire Barrier	M	Building walls provide a fire and heat barrier between the room and outside
EC-7	Bldg Fire Protection System	M	Building contains automatic initiation of fire suppression sprinklers with thermal valves. These valves open at about 100°C. There are fire alarms providing notification throughout the facility. These alarm circuits are designed fail-safe.
EC-8	Tritium Monitoring System	M	The facility has tritium monitors to monitor for airborne tritium in the workspace and the HVAC stack.
EC-9	LN ₂ auto flow control shutoff	M	Monitors LN ₂ flow and initiates valve shutoff, causing flow interrupt when abnormal flow occurs.
EC-10	Building Structure	P, M	Building structure is designed to control HVAC airflow into, through, and out of the building, in combination with the HVAC
EC-16	HVAC	M	The HVAC system provides heating, ventilation, and air conditioning and pressure differential for the building. The design controls air flow, forming a differential pressure, so that the air flows from occupied to laboratory areas and out through the stack.
EC-17	DOT Trailer	M	The tube trailer is DOT certified for over-the-road use. This certification ensures the tube design is qualified to contain the gas at its storage pressures with a margin of safety and that the tubes are secured to the trailer.
EC-23	DOT Type B Shipping Containers	M	DOT shipping containers have robust design and meet federal specification that include impact, drop, and fire.
Administrative Controls			
AC-1	Combustion Control Program	P	The Combustion Control Policy limits the amount of fuel material inside or outside the building.
AC-13	Inventory Control	M	The facility will have an inventory control program that limits the material to less than XX.
AC-8	Trained Escort	M	Construction workers will be escorted by person(s) having radiation worker training and some knowledge of the facility.

During the previous organization of the HA, linking activities to the process segments usually reveals redundancies. For example, material may be machined, melted, sintered, etc in a number of locations using similar equipment. When the HA evaluates each activity, the listing of scenarios of redundant activities can usually be accomplished by simple ‘cut and paste’. It is important not to delete these repeated scenarios but to include them wherever they are identified, serving to point out that controls that continue to be repeated may have a higher level of importance.

For each postulated accident scenario the scribe will document the scenario number, hazard, accident type, and the accident description, most likely on a blank results table to be later processed into the final results table (see table 8).

Identify Control Features (Columns 7 & 8)

Both the preventative features that could have a significant effect on the accident frequency and the mitigative features that could reduce the consequences on an accident need to be identified. These identified controls can be either engineered systems, administrative, or passive. As these controls are identified throughout the HA, the scribe will develop the companion ‘controls table’ (see Table 9) for later use. Any additional control that the team feels could be effective or needed is also recorded. During this exercise, the scribe should also indicate on the results and controls tables whether the specific control is primarily (1) preventive or (2) mitigating in nature.

Unmitigated and Mitigated Frequency Assessment (Columns 5 & 9)

Initially assess the frequency bin of each identified accident scenario with no controls (i.e., unmitigated). This is the frequency bin of the event as it is developed in the hazard/accident scenario discussion. Then assess the accident frequency when credit is taken for the identified controls. Safety analysts are valuable at this stage to provide data or experience in estimating frequencies. These analysts should be able to judge the effectiveness in reducing the likelihood of the accident if the control(s) identified are in place. Operators are also helpful as they can indicate if a postulated failure, event, or initiator has actually occurred. They also can provide insight into how many redundant controls should be considered. For example, if there are more than 2 or 3 administrative controls to prevent human errors, then only a couple can be really counted on as in human situations if the first several fail, there is generally known to be a common cause human failure that prevents the others from being effective.

Some typical guidelines are as follows:

- Administrative controls (ACs) reduce the scenario frequency by a factor of 10. If there are two or more independent ACs, a maximum of two orders of magnitude reduction (one frequency bin) in scenario frequency can be assumed
- Engineering controls that have surveillance requirements are assumed to reduce the frequency by a factor of 100 (one frequency bin), unless there is specific data available for the control.

The accident scenario frequencies are qualitative and based primarily on engineering judgment. When available, site-specific data may be used if it provides added insight. Normally, the team should retain the detailed handwritten data for each scenario, or document in a word processing form, these details. The retained information is useful if reviewers need to understand the rationale for consequence or frequency estimates or if the HA is to be revised in the future.

Unmitigated and Mitigated Consequence Assessment (columns 6 and 10)

The criteria provided by matrices shown in Tables 4 and 5 are to be used to assess the consequences of each identified accident scenario for the public and workers respectively. The tables provide quantitative consequence bins for nuclear and chemical hazards and a qualitative description to be used for other hazards (e.g. high explosives). Initially assess the consequence bin of the accident with no control measures (unmitigated).

For the public and the worker the unmitigated consequence takes no credit for any mitigative features including passive design features. Next determine the mitigated consequences. This would include passive features (e.g., primary confinement like the containers or packaging holding the material, exterior walls of the structure, fire walls, HEPAs, etc.), and active features (e.g., ventilation, fire suppression and detection, etc.).

This approach is obviously very conservative; however, more detailed analysis can be done when doing the accident analysis. The point here is to make sure a consistent approach is followed so that it is possible to get a relative comparison of the accident scenario consequences. By determining the totally unmitigated consequences, we also determine which accidents must rely on controls. If the worst possible, or unmitigated, consequences are low then we would then know that formal controls are not required.

Attachment B provides guidance for estimating the public consequences for radiological releases. There have been attempts to provide similar guidance for calculating worker consequences, however, no such guidance is provided here. Most senior analysts recognize the difficulty and, too often, the errors in calculating worker consequences. There are many uncertainties, for example, in calculating worker doses in a small confined area such as a laboratory as to make the exercise essentially useless. Parameters such as HVAC airflow, air flow patterns, ability of the workers to evacuate, specific conditions of the material being releases such a aerodynamic diameter and density, etc. tend to be the drivers. A qualitative assessment by the safety analysts and operational team members of worker consequences is considered much more accurate than calculations.

Conversely, concentrations of airborne material at distances associated with the public (hundreds of meters) calculated either by simple hand calculations or bounding computer code calculations are seen as very useful and more accurate for those receptors at farther distances. Hence the rationale for Attachment B. For public consequences, previous calculations or results of modeling may be used if they are appropriate to the analysis boundary conditions and other assumptions.

3.2.3 Hazard Evaluation and Selection of Formal Controls

Analysts and facility management/operating staff should realize that the ultimate goal of any successful safety analysis process is to assure that the appropriate controls are in place and maintained effectively. While there are usually redundant controls that can prevent or mitigate hazardous situations there may be only a few that are really effective. In those cases, it is appropriate to formalize those controls so as to assure they are in place under all conditions in which they are needed. Higher levels of quality may also be required when designing, constructing, maintaining, or operating hardware or systems that are formally controlled.

For an HA associated with a DOE STD 3009 safety analysis, Chapter 3 of the SAR as defined in the 3009 format and content, requires an evaluation of the results of the HA to first determine if there are safety significant SSCs and controls that are necessary for worker protection. Defense in Depth SSCs and controls may also be selected. If an accident analysis is then performed, further selection of safety class SSCs and controls is performed for public protection. Ultimately, these Safety SSCs, are then controlled by formal Technical Safety Requirements. If the HA is prepared for a Standard 3009 SAR, the requirements of Chapter 3 of DOE standard 3009 should be followed. This handbook provides acceptable methods to be used in conjunction with 3009.

While it is beyond the scope of this Handbook to provide a prescriptive recipe to hazard evaluation and selection of formal safety controls, there is general guidance that is appropriate. Attachment C provides some general guidance to be used in this process. Note that because this part of the process is not prescriptive and well defined, it is primarily a process of using sound and objective engineering and management judgement based on the results of the HA.

Due to its interpretative nature, there can be divergent views among the involved parties. It is imperative that communications remain open and professional, and that an ongoing dialogue occurs among involved parties at various stages of the process. The following is suggested:

- The HA team leader/analysts meet with facility management to review the results of the HA and those controls that the HA team may recommend for elevation to ‘safety’.
- Facility management (SB project leader) meet with the approving authority to discuss selection of safety controls. It is better to gain agreement as early as possible so that documentation only needs to occur once. For non-nuclear facilities, the FM would meet with the FWO-OAB. For nuclear facilities the FM would meet with DOE LAAO.

Ultimately the FM is responsible for maintaining the selected safety controls. See Attachment C for additional guidance for evaluating the HA results and selecting safety level controls.

3.2.4 Format and Content for Standalone Hazard Analysis

In many cases the HA is part of the analysis required for a non-reactor nuclear facility SB. In that case the HA that is performed will be integrated into the documentation and evaluation required under the format and content of STD 3009.

In the event that the HA is to be a standalone evaluation used for approval purposes for an activity, operations, or facility not a part of a STD 3009 analysis, the analysis and its results must be documented in a comprehensive and defensible manner. The document must provide to the approval authority:

- a complete scope of the analysis,
- a full identification and evaluation of the hazards,
- identification of all of the available controls, and
- selection of those controls that are most important

These last controls are normally given a term, e.g. ‘Controls Important to Safety’, ‘Major Contributors to Safety’, ‘Defense in Depth’, etc that denotes control with a higher level of formality, quality assurance and commitment. This normally establishes a ‘safety basis’ which, if

the conditions cannot be met, actions must be taken to restore the control to its effectiveness or place the operation in a safe configuration, e.g. shutdown the operation or place in a safer mode.

For a standalone HA the following format and content is suggested as a defensible starting point. This is consistent with the requirements for a documented safety analysis (DSA) as described in 10CFR830 and its Implementation Guides.

Suggested Format and Content (Abbreviated)

Executive Summary (optional)

1. Site Description
 - a. Brief summary of location, other LANL facilities, etc
 - b. Natural Phenomena summary (meteorology, seismology, flood plains, etc)
2. Description of Facility and Operations
 - a. Facility and Site Description
 - b. Facility Systems, Structures, and Components
Describe in detail those SSCs that are determined to be ‘major contributors to safety’ or ‘defense in depth’ based on the hazard evaluation, below
 - c. Facility Operations
3. Hazard Analysis
 - a. Hazard Identification
 - b. Hazard Analysis
 - c. Hazard Evaluation
Evaluate all of the highest consequence accidents and the available controls to determine those that are of most importance, and that should be classified at the higher levels of safety(major contributors to safety, etc)
4. Identification of Important Controls
 - a. Controls that are “Major Contributors to Safety”
 - b. Controls that are “Defense in Depth”
Describe the formal mechanisms in place to assure the effectiveness of these controls
5. Safety Management Programs
Describe those programs that are important for safety to the workers, public, etc.

3.3 Preliminary Hazard Analysis for Project Design Phase

For construction project, a Preliminary Hazard Analysis (PHA) is a useful tool that should be performed during the early design stages. LIR-220-01-01, Construction Project Management, identifies requirements for a PHA to be performed at the pre-conceptual or conceptual design phase. The PHA is necessary to accomplish a number of critical steps, among which are the following:

1. Identifies facility hazards and engineering controls
2. Determine facility hazard category
3. Identify safety class or safety significant SSCs
4. Identifies quality level for safety SSCs and the facility structure
5. Identifies safety function, functional requirements, and design criteria for safety SSCs

6. Input to other key project documents, e.g. Functional and Operational Requirements.

At this design stage the project team should only be concerned with identifying the engineering features, not administrative controls, associated with the project. Because the PHA is performed early in design, engineering controls are to be maximized in order to have less reliance on administrative controls during the operational phase. Note that the PHA and the Project Functional and Operational Requirements (F&OR) are complementary documents. The F&OR is used for input to the PHA, then however, the PHA results are either confirmatory for the F&OR or may result in changes to that document.

The Project Leader should identify a PHA team leader and/or safety analysts as early as possible in order that safety staff are available and an integral part of the project team. In performing the PHA, the steps in Section 3.1, Pre-Start Activities are applicable, however, there is more emphasis on design of the structure, engineering features, and SSCs at this stage. Baseline information may be gathered for other facilities that are similar to the one being designed. The activity and layout of the facility being considered is important. Equally important is completion of the Hazard Identifications Checklist (Attachment A).

In order to provide a consistent framework, design oriented PHA tables are provided along with a description of the process of completing the tables. Table 10, PHA Results Table, and Table 11, SSC Safety Functions and Design Criteria should be completed for all design phase PHAs. These tables should be adapted to the project in a manner that works best.

3.3.1 PHA Results Format

Using all of the information developed by the section 3.1 pre-start activities, the PHA team, conducts its interactive team sessions to identify potential accidents and their consequences, using the What If methodology. Table 10 is completed. The example which follows lists types or classes of accidents, I thought VII, such as 'Operational Fires' and 'Loss of Confinement'. Most facilities have in common these classes of accidents. If there are classes of accidents of a different nature or if there is a more logical way to break the classes of accidents, the PHA Team should do so.

1. "What IF Question" (column 1). A brief statement of the question with the results, similar to an initiator and the resulting actions. For example under 'I. Operational Fires', the first scenario could be, '1. Hydraulic fluid from the forklift leaks and ignites a fire inside the drum storage area'.
2. Unmitigated Consequences (column 2). Provide a brief qualitative statement as to the results of the accident described in the 'What If' column. Does the resulting accident impact the public, worker, or environment. Perform a qualitative assessment of the level of the consequences and list the consequence bin from Table 2 or 3.
3. Preventive Features (column 3). List design features that would prevent the accident, e.g. equipment design that prevents a fire (e.g. forklift without flammable fuel source). List the name in a manner that is logical and to be used for future references to this SSC.
4. Mitigative Features (column 4). List any design features that would mitigate the accident, e.g. HVAC with filters that minimize the release outside the facility.
5. Comment or Action Items (column 5). List any comments or further actions to consider.

Note: In addition to Table 10, a companion listing of all of the engineering features should be constructed, similar to the example in Table 9. The companion table is merely a complete listing of all of the engineered SSCs and features from table 10.

3.3.2 SSC Safety Functions and Functional Requirements

Table 11 becomes a listing of each of the engineered features that is identified in the PHA, as derived from the PHA results in Table 10 and the companion table that is a listing of all engineered features. Complete Table 11 as follows.

1. Engineered SSC or feature (column 1). Identify the feature or SSC using Table 10 and/or the companion table of all SSCs and features. The final table will have addressed all SSCs and features that were identified in the PHA.
2. Safety Function (column 2). Through inspection of the PHA results table, list all of the safety function of the SSC or feature. For example, not that in Table 11, there are a number of safety functions listed for the building structure, derived from inspection of the PHA results of multiple accidents (What If questions) in Table 10.
3. Functional Requirements (column 3). List the specific functional requirements that are needed to address the safety function(s). The PHA team can make a judgement about the level of safety of the feature, e.g. safety class, safety significant, or defense-in-depth based, based on the unmitigated consequences and safety function.
4. Comment or Action Items (column 5). List any comments of the PHA team or further actions to consider.

The specification of applicable Design Criteria, Codes, and Standards is an important task that should be undertaken by either the PHA Team and/or project design team. The determination of design criteria, codes, and standards should be a follow-on activity. Specific DOE Orders, design codes, or other applicable design requirements may be referenced. For example, a specific National Fire Protection Association (NFPA) code or sections of a code may be referenced for a fire protection system or individual components of the system. The FWO Systems, Engineering, and Maintenance Group (FWO-SEM) should be contacted to assist in this important task.

Table 10 PHA Results Table

Process _____
Preparer _____

Location _____
Reviewer _____

Date _____

Engineered Features

Hazard	What If Question	Unmitigated Consequences (consequence bin from Table 2 or 3)	Preventive Feature	Mitigative Features	Comments or Action Items
	I. Operational Fires				
Radiological Materials (Pu, EU)	1. Hydraulic fluid leaks and ignites inside the drum storage area	<ul style="list-style-type: none"> public exposure to radioactivity (A) worker exposure or injury (A) 	Design of handling equipment inside facility (forklift, etc) Design of containers (drums)	Fire Protection System (alarms, suppression & fire barriers) HVAC with filters	
	II. Explosions or Energetic Events				
	III. Loss of Confinement (spills or leaks)				
	IV. Operational Transients				
	V. Criticality				
	VI. External Events				
	1. Vehicle crashes into loading dock area causing a breach of containers	<ul style="list-style-type: none"> public exposure to radioactivity (B) worker exposure or injury (B) environmental contamination 	Design of loading dock area to prevent interaction of vehicle and containers (e.g. elevated dock area) Design of containers		
	VII. Natural Phenomena				

Table 11. SSC Safety Functions and Functional Requirements

Engineered Feature or SSC	Safety Function	Functional Requirements	Comments
1. Building Structure	<ul style="list-style-type: none"> secondary confinement for operations to withstand all DBAs, natural phenomenon, and external events, provide structural support for essential systems 	<ul style="list-style-type: none"> confine radioactive material released from postulated accidents (safety class) maintain structural integrity during a seismic event required for PC-3 structure (safety class) Maintain integrity when exposed to straight winds of up to 77 mph Provide a 2 hr rated fire barrier (safety significant) 	
2. HVAC with filters			
3. Container for storage of radioactive materials			
4. Fire Protection System <ul style="list-style-type: none"> Alarms Suppression Fire Barriers 			
5. Loading dock structure			
6.			

3.4 Hazard Analysis for Project Title I Preliminary Safety Document

Prior to the startup and operational phase of new facility, a Final Documented Safety Analysis (nuclear facility) or Final Facility Safety Analysis (non-nuclear facility) will be required. A preliminary or draft version of these safety documents will be performed during the project execution or Title I Design phase and available prior to Project Execution (Construction). The Title I document updates previous information that was preliminary in nature. Attributes of the safety document (PDSA or PFSA) at this stage are:

1. Final design information is known, so parameters of engineered SSC and design features can be better described and considered in the analysis.
2. A final definition of safety SSCs can be made (safety class, safety significant, defense-in-depth).
3. Formal safety controls, e.g Technical Safety Requirements (TSRs), can be identified and drafted.
4. Safety management programs can be identified and drafted into the appropriate chapters of the safety document.
5. Administrative controls and other operating procedures can now be identified and considered, although not written or finalized.
6. A draft quantitative accident analysis can be prepared if the HA indicated potential public impacts near the evaluation guideline.

The fundamental baseline for the preliminary safety document, as in most DOE safety analyses, is the Hazard Analysis. Section 3.2 of this handbook described the operational phase HA while section 3.3 described the conceptual design stage HA. The Title I HA builds upon the conceptual design HA with more definitive information and begins to take shape into the format of the operational phase HA. For this reason the HA can be prepared in similar fashion as the operational phase HA.

Simple guidance for this activity is as follows:

1. Select an HA team and team leader as described previously in section 3.1
2. Use the baseline information prepared during the conceptual design HA prepared under the guidance of Section 3.3
3. Initiate team meeting and perform an updated HA, using the format and guidance of section 3.2 for an operational phase HA. Because the conceptual design HA only considered engineered features, the Title I HA now begins to identify operational procedures, safety management programs, and administrative controls.
4. Complete the conceptual design HA, coordinating the reviews and approvals through the project team as required by project plans and appropriate DOE and LANL requirements.
5. Use the conceptual design HA as input into the draft PDSA or draft PFSA required to be completed prior to Project Execution (Construction).

REFERENCES

1. Guidelines For Hazard Evaluation Procedures, Second Edition with Worked Examples, American Institute of Chemical Engineers, 1992.
2. Safety Analysis and Risk Assessment Handbook, , Rocky Flats Environmental Technology Site, Report No: RFP-5098-Pt.1, Rev. 0, April 22, 1997.
3. Hazard and Accident Analysis To Meet Nonreactor Nuclear Facility Safety Analysis Report (SAR) Requirements, a DOE sponsored course by LANL Office of Authorization Basis.
4. Hazard and Accident Analysis Process, Project Hanford Policy and Procedure System, C. Brad Evans, 12/9/97.
5. System Safety 2000, Joe Stevenson, Van Nostrand Reinhold, 1991.
6. DOE Order 5480.23, "Nuclear Safety Analysis Reports," Change 1, US Department of Energy, Washington, DC, March 1994.
7. DOE-STD-3009-94, "Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports," US Department of Energy, Washington, DC, July 1994.
8. 10CFR835, "Occupational Radiation Protection Program," Code of Federal Regulations, US Department of Energy, Washington, DC, January 1998.
9. 10 CFR 830, Nuclear Safety Management, subpart B, Safety Basis Requirements. January 2001.
10. 29 CFR 1910.119, "Subpart H—Process Safety Management of Highly Hazardous Chemicals," Occupational Safety and Health Administration, Washington, DC, July 1998.
11. 40 CFR 61, "National Emission Standards for Hazardous Air Pollutants," Subpart H, "National Emission Standards for Emissions of Radionuclides Other Than Radon From Department of Energy Facilities," US Environmental Protection Agency, Washington DC, July 1998.
12. DOE Order 420.1, "Facility Safety" Change 2, US Department of Energy, Washington, DC, October 1996. Only applicable sections are Paragraphs 4.4 through 4.4.6.
13. DOE Order 5400.1, "General Environmental Protection Program," Change 1, US Department of Energy, Washington, DC, June 1990.
14. DOE Order 5400.5, "Radiation Protection of the Public and Environment," Change 2, US Department of Energy, Washington, DC, January 1993.
15. DOE-STD-1020-94, "Natural Phenomena Hazards Design and Evaluation Criteria for DOE Facilities," Change 1, US Department of Energy, Washington, DC, January 1996.
16. DOE-STD-1027-92, "Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports," Change 1, US Department of Energy, Washington, DC, September 1997.
17. 1994 Uniform Building Code, International Conference of Building Officials, 1994.

Attachment A: Hazard Identification Checklist³

Hazard	Description (Form, Quantity, Packaging)	Location
Acceleration <ul style="list-style-type: none"> • Inadvertent Motion • Sloshing of Liquids • Translation of loose objects 		
Deceleration <ul style="list-style-type: none"> • Impacts (sudden stops) • Failing of brakes, wheels, tires, etc • Falling objects • Fragments or missiles 		
Chemical Reaction (nonfire) <ul style="list-style-type: none"> • Disassociation, product reverts to separate components • Corrosion, rust, etc • Combination, new product formed from mixture 		
Electrical <ul style="list-style-type: none"> • Shock • Burns • Overheating • Ignition of combustibles • Inadvertent activation • Explosion, electrical • Static, electrostatic electricity 		
Explosions <ul style="list-style-type: none"> • Commercial explosive present • Explosive gas • Explosive liquid • Explosive dust 		
Flammability and Fires <ul style="list-style-type: none"> • Presence of fuel – solid, liquid, gas • Presence of strong oxidizer – oxygen, peroxide, etc. • Presence of strong ignition force – welding torch, heaters 		
Heat and Temperature <ul style="list-style-type: none"> • Source of heat, non-electrical • Hot surface burns • Very cold surface burns • Increased gas pressure caused by heat • Increased flammability caused by heat • Increased volatility caused by heat • Increased activity caused by heat 		

³ Guidelines for Hazard Evaluation Procedures, AiChe, 1992, Table 6.11

Hazard	Description (Form, Quantity, Packaging)	Location
Mechanical <ul style="list-style-type: none"> • Sharp edges or points • Rotating equipment • Reciprocating equipment • Pinch points • Weights to be lifted • Stability/toppling frequency • Ejected parts or fragments 		
Pressure <ul style="list-style-type: none"> • Compressed gas • Compressed air tool pressure system exhaust • Accidental release • Objects propelled by pressure • Water hammer • Flex hose whipping 		
Static <ul style="list-style-type: none"> • Container rupture • Overpressurization • Negative pressure effects 		
Leak of material <ul style="list-style-type: none"> • Flammable • Toxic • Corrosive • Slippery 		
Radiation <ul style="list-style-type: none"> • Ionizing Radiation • Ultraviolet radiation • High intensity visible light • Infrared radiation • Electromagnetic radiation • Laser radiation 		
Toxicity <ul style="list-style-type: none"> • Gas or liquid • Asphyxiant • Irritant • Systemic poison • Carcinogen • Mutagen • Combination product • Combustion product 		
Vibration <ul style="list-style-type: none"> • Vibrating tools • High noise source level • Mental fatigue • Flow or jet vibration • Supersonics 		

Attachment B: Estimating Accident Scenario Public Radiological Consequences

This section provides a method to estimate the consequences of radiological releases to the public or receptors that are on the order of hundreds of meters or more from the release point. This need be done only for a couple of cases, involving the highest inventory of material at risk (MAR). Subsequent accidents involving lesser materials can be judged accordingly. The method below is intended to be a conservative, hand calculation, i.e., not a modeling effort by an analyst using computer codes. This method below has enough precision to select the appropriate public consequence bin, but does not replace the accident analysis that will be performed after the HA.

Down-wind consequences from a radiological release are expressed as a dose in units of rem (roentgen-equivalent-man). Usually, down-wind doses are due to inhalation and that is the exposure mode described here, with very little contribution from direct radiation exposure. One must consider, however, that in the case of radioactive noble gases that are not absorbed readily by inhalation that the major dose contribution comes from cloud-shine rather than inhalation, a situation that is not likely at LANL.

For inhalation, the dose is calculated as:

$$Dose(rem) = \sum_i [ST_i(g) * DCF_i(rem/g) * BR(m^3/s) * \chi/Q(s/m^3)]$$

where:

- Dose = CEDE or 50 year committed effective dose equivalent, dose the uptake commits the individual to over a 50 yr span
- ST = source term
- DCF = dose conversion factor
- BR = breathing rate
- χ/Q = atmospheric dispersion factor
- I = the radionuclide

Since radiation effects are additive, the dose is calculated for each radionuclide and the doses added.

Source Term:

The source term is the amount of respirable material released to the atmosphere. Units can be either mass (grams) or activity (curies). Whatever the units, they need to be consistent with the units used for the dose conversion factor (DCF) in the following term.

The source term is determined by:

$$ST(g) = MAR(g) * DR * ARF * RF * LPF, \text{ commonly referred to as the "five-factor formula"}$$

where: MAR = material at risk

DR = damage ratio

ARF = airborne release fraction

RF = respirable fraction
LPF = leak path factor

The MAR is the quantity of a radionuclide subject to influence by the accident initiator. For a major building fire, it may be the entire building inventory. For operational upsets, it will be only the quantity of material involved in that operation.

The DR is the fraction (dimensionless) of the MAR actually released by the accident scenario, normally judged to be 1 for most unmitigated scenarios.

The ARF is the fraction of the released MAR that becomes airborne and the RF is the fraction of the airborne material that is respirable. Respirable is defined as particles with a mean aerodynamic diameter less than 10 microns. The aerodynamic diameter is related to the geometric diameter by:

$$D_A = D_G * \sqrt{\rho}$$

So, dense particles are more readily deposited in the upper (nasal-pharyngeal) regions and must be smaller in diameter than lighter particles to get to the deeper regions of the lung where they are more readily absorbed.

Help in estimating ARF and RF can be obtained from DOE Handbook, DOE-HDBK-3010-94, "Airborne Release Fractions/Rates and Respirable Fractions for Nonreactor Nuclear Facilities".

The LPF is the fraction of respirable particles released that actually makes it to the outside environment. It is usually taken to be 1.0 for all unmitigated cases because it is usually difficult to defend a smaller value.

Dose Conversion Factor:

Since this guidance addresses only dose by inhalation, the dose conversion factor for effective dose equivalent by inhalation is used. These values are radionuclide-specific and can be obtained from ICRP-30 ("Annals of the ICRP; Limits for Intakes of Radionuclides by Workers") or, more conveniently from "Federal Guidance Report No. 11, Limiting Values of Radionuclide Intake and Air Concentrations and Dose Conversion Factors for Inhalation, Submersion, and Ingestion". Dose conversion factors in these publications use the international units of sieverts (Sv) and becquerels (Bq) so conversion of units is necessary. There are 100 rem/Sv and 3.7×10^{10} Bq/Ci.

Breathing Rate:

This is the breathing rate of the person receiving the exposure and is taken from ICRP-23, "Report of the Task Group on Reference Man". The value for a man engaged in light activity is used, which is 20 liters/min or 3.33×10^{-4} m³/s.

Atmospheric Dispersion Factor:

This is the parameter that expresses the amount of dispersion resulting from down-wind transport. The primary reference for how this value is determined is Appendix A of DOE-ST-3009-94, which

in turn references parts of Regulatory Guide 1.145 by the U.S Nuclear Regulatory Commission. The methodology is a gaussian dispersion model incorporating a statistical treatment of site-specific meteorological data and site-specific distances to off-site locations.

This analysis has been performed for the major nuclear facilities at Los Alamos and the results are tabulated in Table A-1. The table assumes the “parking lot” assumption and uses the ground level (0 meters) release values. A detailed explanation of how these numbers were derived is available in "Atmospheric Dispersion Modeling for Radiological Accident Analyses at LANL Nuclear Facilities", by G. Heindel.

Table A-1 Estimates for χ/Q for LANL Technical Areas

Technical Area	Atmospheric Dispersion Coefficient (χ/Q) for Surface Release Based on 95% tile Distribution (sec/m ³)
TA-3	8E-5
TA-8	1E-4
TA-16	2E-4
TA-18	1E-4
TA-21	3E-4
TA-48	9E-5
TA-50	6E-5
TA-53	1E-4
TA-54 (Area G)	9E-4
TA-54 (RANT)	4E-4
TA-55	6E-5

Attachment C: Guidance for Hazard Evaluation & Selection of Safety Controls

Chapter 3 of DOE Standard 3009 (Ref. 7) provides some guidance on how to evaluate the results of the HA for a non-reactor nuclear facility and then to provide adequate documentation. However, that guidance is not prescriptive and may not be clear for those who are unfamiliar with the process. This attachment is intended to provide additional guidance, however, it should not be viewed as prescriptive but as a set of good practices that have been found to be acceptable. The FWO Office of Authorization Basis may be contacted for further information as needed.

Typically, the HA results as documented in the HA tables identify a wide range of accidents that can impact the workers and public with varying levels of consequence. For hazard evaluation purposes, one is normally most interested in assuring that formal controls are in place to prevent or mitigate those high consequence accidents. High consequence accidents are normally considered to be those in the 'A' or 'B' consequence bins for the public or worker, defined in Tables 3.1.4-2 and 3.1.4-2, respectively. At the end of the HA process, the analysts normally will sort the accidents and identify those accidents in the 'A' and 'B' consequence bins, separating those for the worker and public.

A table of these high consequence accidents might be formatted as follows, taking the worker evaluation first. The analysts would manually or electronically sort the accidents, then identify the appropriate controls and build the table.

Accidents with Worker 'A' or 'B' Consequences	Controls Identified (SSCs, Admin, Passive)						
	A	B	C	D	E	F	G
Accident 1 (e.g. Building Wide Fire)	X	X	X		X		
Accident 2 (e.g. Major Process Spill)			X	X	X	X	
Accident 3 (e.g. Process Explosion)			X	X	X		
Accident 4		X	X	X	X		X
Accident 5			X		X		
Accident 6	X		X				
Accident 7	X		X		X		
Accident 8	X		X				
Accident 9			X		X		
Accident 10						X	X

Normally, inspection of the table above along with supporting information would be all that is necessary to make informed engineering judgements. There are almost always a large number of 'candidate' controls to be considered when selecting those to be formalized as 'safety'.

Some of the criteria developed for a 3009 analysis, as taught in a recent DOE sponsored workshop (Ref. 3) are listed below. These criteria are appropriate for any HA. When selecting specific controls from the candidate list choose those that:

- Reduce risk the most
- Have the most redundancy
- Are preventive over mitigative
- Are passive over active
- Have the fewest active features
- Cover independent mechanisms
- Cover each release pathway
- Have the fewest support systems
- Have functional diversity
- Are easiest to maintain
- Have the fewest surveillances
- Are the least costly

In the above example table of accidents and controls, the analysts by inspection might make the following conclusions. Note however, the table alone does not provide the supporting details. The analysts will want to look at the effectiveness of controls in reducing the likelihood or consequences.

1. Controls 'C' and 'E' are shown to be effective for almost all of the accidents, so it is reasonable to consider those for elevation to 'safety'. Both might be selected for redundancy.
2. For accident #10, neither 'C' or 'E' are effective, leaving only controls 'F' and 'G'. One or both of these would be selected for elevation to 'safety' using the criteria stated above. For example, control 'F' may be much more effective in reducing the accident risk, or it may be preventative, passive, or have several of the better attributes over 'G'. Therefore 'F' would be chosen as 'safety'.
3. The remaining controls might be selected for 'defense-in-depth' since they provide additional layers of protection against these high consequence accidents.

The above logic would be documented when selecting those to be 'safety'. Those selected at the highest 'safety' level, whether termed 'important to safety' or 'major contributors to safety' or so on, can then be formalized with the appropriate 'Operational Safety Requirements', 'Technical Safety Requirements' or other appropriate means of formality.

Some examples of the types of controls most often selected as 'safety' are;

- Fire Protection Systems
- HVAC, including HEPA filters,
- Combustible Control limits
- Material At Risk (MAR) administrative limits
- Building structure used as containment or confinement

After completing the above exercise for high consequence worker accidents, the analysts then perform the same exercise for any accidents for high public consequences. There are almost always many fewer, if any, accidents that have high consequences to the public. For nuclear hazard category 3 or non-nuclear Hazard Category B and C, this should always be true. The analysts or facility management should consult with FWO-OAB if there are accidents within this category.